"HTTP状态401 — 身份验证失败：使用SSO时验证SAML消息时出错

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[问题](#)
[解决方案](#)

简介

本文档介绍在使用单点登录(SSO)时，在一段非活动时间后，您会收到“HTTP状态401”错误消息的问题。

先决条件

要求

Cisco 建议您了解以下主题：

- SSO
- Active Directory联合身份验证服务(AD FS)
- CloudCenter

使用的组件

本文档不限于特定的软件或硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

问题

使用SSO时，在一段不活动时间后，您会收到“401”错误，而不是像图中所示提示再次登录。

HTTP Status 401 - Authentication Failed: Error validating SAML message

type Status report

message Authentication Failed: Error validating SAML message

description This request requires HTTP authentication.

Apache Tomcat/8.0.29

您重新登录的唯一方法是关闭整个Web浏览器并重新打开它。

解决方案

这是由于CloudCenter和SSO服务器之间的超时值不匹配引起的。

增强功能允许ForceAuthn参数支持，这允许两个值与CloudCenter之间不匹配以正常注销。此增强功能可在此处跟踪https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvg36752。

唯一的解决方法是消除不匹配。有三个位置需要匹配超时值。前两个是CCM本身。

1. 导航至 /usr/local/tomcat/webapps/ROOT/WEB-INF/web.xml。
2. 修改**<session-timeout>time_In_Minutes</session-timeout>以**反映所需的超时（以分钟为单位）。
3. 导航至 /usr/local/tomcat/webapps/ROOT/WEB-INF/mgmt.properties。
4. 修改saml.**maxAuthenticationAge.seconds=timeout_in_seconds，以**反映所需的超时（以秒为单位）。

第三个是SSO服务器，位置可能因运行的SSO服务器类型而异。Web SSO生存期值必须与CloudCenter上配置的两个值匹配。

一旦全部三个匹配，超时发生后，您将被丢弃回登录屏幕，然后才允许查看该页面。